

LAWRENCE G. WASDEN  
Attorney General

JUDY L. GEIER – ISB No. 6559  
Deputy Attorney General  
State of Idaho  
Department of Insurance  
700 W. State Street, 3<sup>rd</sup> Floor  
P.O. Box 83720  
Boise, Idaho 83720-0043  
Telephone: (208) 334-4204  
Facsimile: (208) 334-4298  
[judy.geier@doi.idaho.gov](mailto:judy.geier@doi.idaho.gov)

FILED  
JAN 17 2017  
Department of Insurance  
State of Idaho

*Attorneys for the Department of Insurance*

**BEFORE THE DIRECTOR OF THE DEPARTMENT OF INSURANCE  
STATE OF IDAHO**

In the Matter of:

ANTHEM INSURANCE COMPANIES,  
INC.

NAIC No. 28207  
Idaho Certificate of Authority No. 2620

Docket No. 18-3269-17

**ORDER ADOPTING REGULATORY  
SETTLEMENT AGREEMENT**

On or about December 6, 2016, the Idaho Department of Insurance (**Department**) received notice of a proposed regulatory settlement agreement concerning Anthem Insurance Companies, Inc. (**Anthem**), an Indiana-domiciled insurer authorized to transact insurance in the state of Idaho pursuant to Idaho Certificate of Authority No. 2620. The Director of the Department (**Director**), having reviewed the same, makes the following findings and conclusions:

1. The Director has jurisdiction in the state of Idaho over matters involving

insurance regulation, pursuant to the Idaho Insurance Code, Idaho Code § 41-101 *et seq.*

2. The insurance regulators for the states of California, Indiana, Maine, Missouri, New Hampshire, North Dakota, and South Carolina (the **Lead Regulators**) undertook a targeted multi-state market conduct and financial examination of Anthem following Anthem's announcement in February 2015 of a specific data breach. The purpose of the examination was to assess Anthem's state of cybersecurity preparedness prior to the data breach, its post-data breach response, the adequacy of measures taken by Anthem to mitigate the harm to consumers whose personally identifiable information was compromised, and to determine the identity of the actors responsible for the data breach. In light of the findings of the Lead Regulators, corrective action taken by Anthem, and additional corrective actions to be taken by Anthem, the Lead Regulators and Anthem have entered into a Regulatory Settlement Agreement (**Agreement**), which is attached hereto as Exhibit 1.

3. The Director finds that the terms of the Agreement are appropriate and adoption of the Agreement is in the best interests of the state of Idaho.

4. The Director having signed the Participating Regulator Adoption Form, attached hereto as Exhibit 2, on December 14, 2016, and the Agreement having become effective on December 31, 2016, based on its adoption by a requisite number of jurisdictions, the Director now wishes to memorialize the Agreement by entry of this order.

NOW, THEREFORE, in consideration of the premises,

**IT IS HEREBY ORDERED** that the Agreement is hereby approved, adopted, and fully incorporated herein by reference. Anthem shall comply with all terms and conditions of the Agreement in accordance with its provisions.

DATED this 17<sup>th</sup> day of January, 2017.

STATE OF IDAHO  
DEPARTMENT OF INSURANCE

  
DEAN L. CAMERON  
Director

**NOTIFICATION OF RIGHTS**

This Order constitutes a final order of the Director. Any party may file a motion for reconsideration of this final order within fourteen (14) days of the service date of this order. The Director will dispose of the petition for reconsideration within twenty-one (21) days of its receipt, or the petition will be considered denied by operation of law. *See*, Idaho Code § 67-5246(4).

Pursuant to Idaho Code §§ 67-5270 and 67-5272, any party aggrieved by this final order may appeal it by filing a petition for judicial review in the district court of the county in which: (1) the hearing was held; or (2) the final agency action was taken; or (3) the aggrieved party resides or operates its principal place of business in Idaho; or (4) the real property or personal property that was the subject of the agency decision is located. An appeal must be filed within twenty-eight (28) days of: (a) the service date of this final order; or (b) an order denying a petition for reconsideration; or (c) the failure within twenty-one (21) days to grant or deny a petition for reconsideration, whichever is later. *See*, Idaho Code § 67-5273. The filing of a petition for judicial review does not itself stay the effectiveness or enforcement of the order under appeal.

### CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 17<sup>th</sup> day of January, 2017, I caused a true and correct copy of the foregoing ORDER ADOPTING REGULATORY SETTLEMENT AGREEMENT to be served upon the following by the designated means:

Anthem Insurance Companies, Inc.  
220 Virginia Avenue  
Mail-Point IN0202-B560  
Indianapolis, IN 46204-3709

☒ first class mail  
☐ certified mail  
☐ hand delivery

California Department of Insurance  
Dave Jones, Commissioner  
300 Capitol Mall, Suite 1700  
Sacramento, CA 95814

☒ first class mail  
☐ certified mail  
☐ hand delivery

Indiana Department of Insurance  
Stephen W. Robertson, Commissioner  
311 W. Washington Street, Suite 103  
Indianapolis, IN 46204-2787

☒ first class mail  
☐ certified mail  
☐ hand delivery

Maine Bureau of Insurance  
Eric A. Cioppa, Superintendent  
34 State House Station  
Augusta, ME 04333-0034

☒ first class mail  
☐ certified mail  
☐ hand delivery

Missouri Department of Insurance  
John M. Huff, Director  
P.O. Box 690  
Jefferson City, MO 65102-0690

☒ first class mail  
☐ certified mail  
☐ hand delivery

New Hampshire Insurance Department  
Roger A. Sevigny, Commissioner  
21 South Fruit Street, Suite 14  
Concord, NH 03301

☒ first class mail  
☐ certified mail  
☐ hand delivery

North Dakota Insurance Department  
Jon Godfread, Commissioner  
600 E. Boulevard Avenue, 5<sup>th</sup> Floor  
Bismarck, ND 58505-0320


☒ first class mail  
☐ certified mail  
☐ hand delivery

South Carolina Department of Insurance  
Raymond G. Farmer, Director  
P.O. Box 100105  
Columbia, SC 29202-3105

☒ first class mail  
☐ certified mail  
☐ hand delivery

Judy L. Geier  
Deputy Attorney General  
Idaho Department of Insurance  
700 W. State Street, 3<sup>rd</sup> Floor  
P.O. Box 83720  
Boise, ID 83720-0043

☐ first class mail  
☐ certified mail  
☒ hand delivery

  
Pamela Murray



## REGULATORY SETTLEMENT AGREEMENT

This Regulatory Settlement Agreement (“Agreement”) is entered into this \_\_\_th day of December 2016, by and between Anthem Insurance Companies, Inc. (“Anthem” or the “Company”), and the California Department of Insurance, Indiana Department of Insurance, Maine Bureau of Insurance, Missouri Department of Insurance, New Hampshire Insurance Department, North Dakota Department of Insurance, and South Carolina Department of Insurance (collectively, the “Lead Regulators”) and the insurance regulatory departments, divisions, or offices of each of the remaining States and U.S. jurisdictions that adopt, agree to, and approve this Agreement (the “Participating Regulators”).

### A. Recitals

1. Anthem is the nation’s largest health benefits company by membership, licensed to conduct business in all fifty States and the District of Columbia. It maintains its home office in Indianapolis, Indiana, and markets products and services in many jurisdictions using either in its own name or the name and marks of Blue Cross Blue Shield, UniCare, CareMore, and Amerigroup.

2. On February 5, 2015, Anthem announced a specific data breach. That data breach was the result of an attack that began surreptitiously on February 18, 2014, and led to exfiltration of personally identifiable information (“PII”), including names and (in some cases) social security numbers, of 78.8 million consumers beginning in December 2014 (“Data Breach”). The Data Breach was discovered on January 27, 2015, and the last successful malicious activity was noted by Anthem on January 30, 2015.

3. The Lead Regulators are the Lead States in a targeted multistate market conduct and financial examination (“Examination”) initially called by the Indiana Department of Insurance as lead domestic regulator on February 26, 2015. All other states and U.S. jurisdictions belonging to the National Association of Insurance Commissioners participated in the Examination. The purpose of the Examination was to assess Anthem’s state of cybersecurity preparedness prior to the Data Breach, its post-Data Breach response, the adequacy of measures taken by the Company to mitigate the harm to consumers whose PII was compromised, and determining the identity of the actors responsible for the Data Breach.

4. The Lead States engaged Alvarez & Marsal Insurance and Risk Advisory Services, LLC (“A&M”) and CrowdStrike Services, Inc. (“CrowdStrike”) to assist in the Examination. Anthem worked cooperatively with A&M and CrowdStrike throughout the examination. On July 20, 2015, A&M and CrowdStrike produced confidential preliminary examination findings to the Lead Regulators.



5. Based on these preliminary findings (and following the Lead States' continuing dialogue with the Company and collaboration with other regulators), A&M produced a public examination report on December 1, 2016 ("Examination Report"). A copy of the Examination Report is attached hereto as Exhibit A. Key findings in the Examination Report include the following:

(a) Anthem's pre-breach cybersecurity was reasonable and included the implementation of technologies and procedures consistent with or exceeding those of a typical organization of its size and type;

(b) Anthem's preparations to respond to a data breach began well before the incident occurred and included a detailed Incident Response Plan ("IR Plan");

(c) The Company's IR Plan allowed it to timely and effectively respond to the Data Breach when it was discovered, removing the attacker's ability to access the network within three days of identifying the Data Breach;

(d) The examiners have identified the attacker with high confidence and concluded with medium confidence that the attacker was acting on behalf of a foreign government. Attacks associated with this foreign government have not resulted in PII being transferred to non-state actors;

(e) Anthem promptly communicated and cooperated with law enforcement and regulatory officials. The Company also provided affected individuals with notice through direct mailing, e-mailing, news publications, website notice, and working with State insurance departments;

(f) Within two weeks of discovering the Data Breach, Anthem contracted with a vendor to provide credit protection services for two years to breach-impacted consumers; and,

(g) Immediately following discovery of the Data Breach, Anthem engaged expert consultants to investigate the Data Breach and assist the Company with its post-breach response.

6. The Lead States have discussed the preliminary findings with the Company as well as Anthems' response to the Data Breach, improvements to its security posture going forward, and its plans for remedial action. To date, the Company has already incurred significant costs related to the Data Breach: \$2.5 million to engage expert consultants; \$115 million for the implementation of security improvements; \$31 million to provide initial notification to the public and affected individuals; and \$112 million to provide credit protection to breach-impacted consumers. The Company and the Lead States have also agreed upon additional security enhancements and further efforts to assist breach-affected individuals.

7. In light of the facts set forth in the confidential preliminary findings and the public Examination Report, the corrective actions already implemented by the Company, and the Additional Corrective Actions described in Paragraph D below, the Lead Regulators find that administrative fines or penalties are not warranted. Considering the Company's pre-breach security posture, its timely and effective response, and the large costs already incurred by Anthem, the Lead States feel any additional monies are better spent on investments in cybersecurity, the maintenance and upgrade of technology, and continuing consumer remediation than on punitive or exemplary fines.

8. The Company is prepared to undertake Additional Corrective Actions in addition to the work already performed, the additional security measures already implemented, and the costs already incurred in responding to the Data Breach.

9. In view of the foregoing facts and circumstances, the Lead Regulators and the Participating Regulators find it to be in the public interest and are willing to accept this Agreement to settle all insurance regulatory matters within the scope of the Examination. The Company believes that such a settlement is in its best interest.

**B. Location of Definitions**

The terms listed below are defined within the Agreement. For convenience, those definitions can be found as referenced below.

- (a) "A&M" is defined in paragraph A.4.
- (b) "Additional Corrective Actions" are those actions described in paragraph D.
- (c) "Affected Minors" is defined in paragraph D.3.
- (d) "Agreement" is defined in the preamble paragraph.
- (e) "Anthem" is defined in the preamble paragraph.
- (f) "Anthem Minor Credit Protection Program" is described in paragraph D.3.
- (g) "Applicable Consent Order" is defined in paragraph E.4(a)
- (h) "Company" is defined in the preamble paragraph.
- (i) "CrowdStrike" is defined in paragraph A.4.
- (j) "Data Breach" is defined in paragraph A.2.
- (k) "Examination" is defined in paragraph A.3.
- (l) "Examination Report" is defined in paragraph A.5.
- (m) "IR Plan" is defined in paragraph A.5(b).
- (n) "Lead Regulators" is defined in the preamble paragraph.



- (o) “Participating Regulators” is defined in the preamble paragraph.
- (p) “PII” is defined in paragraph A.2.

**C. List of Exhibits**

Exhibit A ..... Examination Report dated December 1, 2016  
Exhibit B ..... Exemplar Minor Credit Protection Program Mailing  
Exhibit C ..... Participating Regulator Adoption Form

**D. Additional Corrective Actions**

1. Continued Implementation of Enhanced Security Measures. Anthem has discussed with the Lead Regulators the recommendations of its expert consultants and its plans to continue the installation of enhanced security measures. The Company will complete the work described to the Lead States at an estimated additional cost of at least \$30 million.

2. Continuation of Cybersecurity Monitoring. Anthem engaged outside consultants to conduct ongoing monitoring of its systems. The Company completed the work contemplated by that engagement, has acquired additional tools and hired additional staff to insource this capability, and will continue its heightened monitoring.

3. Anthem Minor Credit Protection Program. Anthem estimates that the Data Breach impacted at least twelve million individuals who were under the age of eighteen when the breach was discovered on January 27, 2015 (“Affected Minors”). This group of underage persons is less likely than others to engage in credit transactions and thus less likely to promptly discover any fraudulent activity. Affected Minors will therefore receive substantial benefits from credit protections similar to that known as a credit “freeze.” The Lead Regulators have therefore asked and Anthem has agreed to provide a credit protection program functionally equivalent to a credit freeze to Affected Minors. Specifically, Anthem will:

(a) Notify the parents or legal guardians of Affected Minors of the availability of the Anthem Minor Credit Protection Program by means of a plan which incorporates a U.S. Mail notice, media notice, website notice, and member portal notice in coordination with the Lead Regulators. The content of the U.S. mail notice will be mutually agreed by the Company and the Lead Regulators and substantially consistent with the Exemplar Minor Credit Protection Program Mailing (attached as Exhibit B). Notification by U.S. Mail will begin in February 2017 and be completed within ninety (90) days thereafter;

(b) Work with the three major credit bureaus (Equifax, Experian, and TransUnion) to, upon request by the parents or legal guardians of Affected Minors, provide for a one-time placement and permanent removal of the Anthem Minor Credit Protection Program for each Affected Minor;

(c) Anthem will pay all costs associated with the Anthem Minor Credit Protection Program for Affected Minors; and,

(d) Anthem will make this offer available for a period of one year after the date of the notice letter.

The estimated cost of implementing the Anthem Minor Credit Protection Program is expected to exceed \$15 million.

**E. Miscellaneous**

1. Effectiveness. This Agreement shall become effective when signed by the Company and the Lead Regulators and adopted by eighteen Participating Regulators through submission of executed Participating Regulator Adoption Forms (attached as Exhibit C).

2. Release. The Lead Regulators and Participating Regulators release and discharge the Company with respect to all damages, fines, claims, sanctions, losses, demands or other liability or redress that each Lead Regulator or Participating Regulator and his or her department could have pursued as a result of the matters falling within the scope of the Examination.

3. No Allegation or Admission. The Lead Regulators have not alleged and Anthem has not admitted any wrongdoing, negligence, or violation of law by the Company.

4. Representations of Authority.

(a) *Lead Regulators and Participating Regulators.* Each person signing on behalf of a Lead Regulator or Participating Regulator gives his or her express assurance that under applicable state laws, regulations, and judicial rulings, he or she has authority to enter into this Agreement. If a Lead Regulator or Participating Regulator finds that, under applicable state law, regulation, judicial ruling, or procedure, the preparation and execution of a consent order or other document is necessary to carry out the terms of this Agreement (the "Applicable Consent Order"), such Applicable Consent Order shall be prepared by the Lead Regulator or Participating Regulator. For purpose of this Agreement, an Applicable Consent Order shall be satisfactory to the Company if it: (i) incorporates by reference and attaches via exhibit a copy of this Agreement, (ii) expressly adopts and agrees to the provisions of this Agreement, and (iii) includes only those other terms that may be legally required in the state of the applicable Lead Regulator or Participating Regulator.

(b) *Company.* The Company expressly represents and warrants as of the date of its execution of this Agreement that: (i) it is duly organized and validly existing and subsisting under the laws of the state of its organization, it is in good standing in such jurisdiction, and neither the execution, delivery, nor performance of this Agreement will violate any law binding on the Company; (ii) it has the full right and power to enter into this Agreement on behalf of the

Company and to perform all obligations hereunder; and (iii) it has obtained all necessary authorizations, approvals, or consents of any governmental entity required in connection with the execution, delivery, or performance by it of this Agreement.

5. Choice of Venue. This Agreement, any disputes which may arise in connection with the interpretation or enforcement of the Agreement, and the rights and obligations of the Parties generally shall be governed by the laws of the State of Indiana without regard or reference to choice or conflict of law rules. The Company, the Lead Regulators, and the Participating Regulators consent to the exclusive jurisdiction of the United States District Court for the Southern District of Indiana or, if such jurisdiction is lacking, the Indiana Circuit Court for Marion County, solely for the purposes of interpreting or enforcing this Agreement and for no other purposes.

6. Waiver. Any agreement on the part of any party hereto to any extension or waiver shall be valid only if in writing signed by the party granting such waiver or extension and shall be a one-time waiver or extension only, and any such waiver or extension or any other failure to insist on strict compliance with any duty or obligation herein shall not operate as a waiver or extension of, or estoppel with respect to, any continuing, subsequent, or other failure to comply with this Agreement.

7. Rights and Remedies. Except as otherwise provided in this Agreement, the rights, powers, remedies, and privileges provided in this Agreement are cumulative and not exclusive of any rights, powers, remedies, and privileges provided by applicable law.

8. Entire Understanding; Modification. This Agreement represents the entire understanding between the parties with respect to the subject matter hereof and supersedes any and all prior understandings, agreements, plans, and negotiations, whether written or oral, with respect to the subject matter hereof. All modifications to this Agreement must be in writing and signed by each of the parties hereto.

9. Execution in Counterparts. This Agreement may be executed in one or more counterparts, any of which shall be deemed an original and all of which taken together shall constitute one and the same Agreement. Execution and delivery of this Agreement may be evidenced by facsimile transmission.

SIGNATURES FOLLOW ON THE SUBSEQUENT PAGE

CALIFORNIA DEPARTMENT OF  
INSURANCE

By: \_\_\_\_\_  
Dave Jones  
Commissioner

Date: \_\_\_\_\_

INDIANA DEPARTMENT OF INSURANCE

By: \_\_\_\_\_  
Stephen W. Robertson  
Commissioner

Date: \_\_\_\_\_

MAINE BUREAU OF INSURANCE

By: \_\_\_\_\_  
Eric A. Cioppa  
Superintendent

Date: \_\_\_\_\_

MISSOURI DEPARTMENT OF INSURANCE

By: \_\_\_\_\_  
John M. Huff  
Commissioner

Date: \_\_\_\_\_

NEW HAMPSHIRE INSURANCE  
DEPARTMENT

By: \_\_\_\_\_  
Roger A. Sevigny  
Commissioner

Date: \_\_\_\_\_

NORTH DAKOTA DEPARTMENT OF  
INSURANCE

By: \_\_\_\_\_  
Adam Hamm  
Commissioner


Date: \_\_\_\_\_

SOUTH CAROLINA DEPARTMENT OF  
INSURANCE

By: \_\_\_\_\_  
Ray Farmer  
Director

Date: \_\_\_\_\_

ANTHEM INSURANCE COMPANIES, INC.

By:  \_\_\_\_\_  
[Name] Thomas Zielinski  
[Position] Executive Vice President and  
General Counsel

Date: 12/2/2016

Report of the

**Multistate Targeted Market Conduct and Financial  
Examination**

for the

<b>California Department of Insurance</b>	<b>New Hampshire Insurance Department</b>
<b>Indiana Department of Insurance</b>	<b>North Dakota Insurance Department</b>
<b>Maine Bureau of Insurance</b>	<b>South Carolina Department of Insurance</b>
<b>Missouri Department of Insurance</b>	

and

**Other Participating Jurisdictions:**

Alabama, Alaska, Arizona, Arkansas, Colorado, Connecticut, Delaware, the District of Columbia,  
Florida, Georgia, Hawaii, Idaho, Illinois, Iowa, Kansas, Kentucky, Louisiana, Maryland,  
Massachusetts, Michigan, Minnesota, Mississippi, Montana, Nebraska, Nevada, New Jersey,  
New Mexico, New York, North Carolina, Ohio, Oklahoma, Oregon, Pennsylvania, Rhode Island,  
South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia,  
Wisconsin, Wyoming, American Samoa, Guam, Puerto Rico, the United States Virgin Islands,  
and the Northern Marianas Islands

of

**Anthem Insurance Companies, Inc. and its Affiliates**

120 Monument Circle  
Indianapolis, Indiana  
NAIC Group # 0671

**December 1, 2016**

## Contents

Letter to Chief Regulators.....	i
Foreword.....	1
Profile of the Companies .....	1
Examination Purpose, Scope, and Structure .....	2
Examination Findings .....	3
Summary .....	7
Verification and Report Submission.....	8
Acknowledgement .....	8
Appendix - Limitations of Report	



December 1, 2016

The Honorable Stephen W. Robertson  
Commissioner  
Indiana Department of Insurance  
311 West Washington Street, Suite 103  
Indianapolis, Indiana 46204-2787

The Honorable Adam Hamm  
Commissioner  
North Dakota Insurance Department  
600 East Boulevard Avenue, 5th Floor  
Bismarck, North Dakota 58505-0320

The Honorable Dave Jones  
Commissioner  
California Department of Insurance  
300 Capitol Mall, 17th Floor  
Sacramento, California 95814

The Honorable Roger A. Sevigny  
Commissioner  
New Hampshire Insurance Department  
21 Fruit Street, Suite 14  
Concord, New Hampshire 03301

The Honorable Raymond G. Farmer  
Director  
South Carolina Department of Insurance  
P.O. Box 100105  
Columbia, South Carolina 29202-3105

The Honorable John M. Huff  
Director  
Missouri Department of Insurance  
Financial Institutions and Professional Registration  
P.O. Box 690  
Jefferson City, Missouri 65102-0690

The Honorable Eric A. Cioppa  
Superintendent  
Department of Professional and Financial Regulation  
Maine Bureau of Insurance  
34 State House Station  
Augusta, Maine 04333-0034

Dear Commissioners Robertson, Hamm, Jones, and Sevigny; Directors Farmer and Huff; and Superintendent Cioppa:

Pursuant to a February 26, 2015 Examination Warrant issued by the Indiana Department of Insurance and the authority granted by CAL. INS. CODE § 730, INDIANA CODE § 27-1-3.1-8, ME. REV. STAT. § 221, MO. REV. STAT. § 374.205, N.H. REV. STAT. ANN. § 400-A:37 N.D. CENT. CODE § 26.1-03-19.2, AND S.C. CODE ANN. § 38-13-10, (the “Examination Statutes”), a targeted multistate market conduct and financial examination was noticed regarding a data breach publicly announced on February 5, 2015 respecting:

**Anthem Insurance Companies, Inc.  
and its affiliated companies**  
(collectively “Anthem” or the “Company”)

The examination was conducted in accordance with the National Association of Insurance Commissioners *Market Regulation Handbook and Financial Condition Examiners Handbook* (“*Handbooks*”), to the extent applicable. The report of examination is herewith respectfully submitted.

Alvarez & Marsal Insurance and Risk  
Advisory Services, LLC

Examiners-In-Charge

## **Foreword**

This report on the multistate targeted examination of the Company is provided pursuant to the *Handbooks*. The principal examination work was conducted by Alvarez & Marsal Insurance and Risk Advisory Services, LLC; Alvarez & Marsal Global Forensic and Dispute Services; and CrowdStrike Services, Inc. (“CrowdStrike”) (collectively, the “Examination Team”).

On February 4, 2015, Anthem notified the Indiana Department of Insurance, its principal domiciliary regulator, that it was investigating a potentially serious data security breach first discovered on January 27, 2015 (“Data Breach”). Anthem also informed regulators that it had retained Mandiant, a cybersecurity consulting firm, to assist the Company with its internal investigation of the incident. The Indiana Department of Insurance then notified the National Association of Insurance Commissioners (“NAIC”) Market Analysis Working Group. Anthem publicly announced the Data Breach on February 5, 2015. On February 26, 2015, the Indiana Department of Insurance advised the Company that a targeted examination had been called to assess Anthem’s state of cybersecurity preparedness prior to the Data Breach, its post-breach response, and the adequacy of measures taken by Anthem to mitigate harm to consumers (“Examination”). Additionally, the Examination Team was asked to determine the identity of the actors responsible for this breach. The Examination was conducted on a multistate basis with Indiana as the Coordinating Lead State, California, New Hampshire, North Dakota, Maine, South Carolina and Missouri as Co-Lead States, and all other members of the NAIC joining as participating jurisdictions.

## **Profile of the Companies**

Anthem is the nation’s largest health benefits company by membership, with member insurers licensed to conduct business in all fifty states and the District of Columbia. The

Company is headquartered in Indianapolis, Indiana, and markets products and services in multiple jurisdictions either using its own name or the name and marks of Blue Cross Blue Shield or affiliates such as UniCare, CareMore, and Amerigroup. The parent company is a publicly traded company.

### **Examination Purpose, Scope, and Structure**

The purpose of the Examination was to assess Anthem's state of cybersecurity preparedness prior to the Data Breach, assess its post-breach response, assess the adequacy of measures taken by Anthem to mitigate harm to consumers, and determine the identity of the actor(s) responsible for the breach (the "Attacker"). The Examination's scope included all U.S. jurisdictions and included the period from February 18, 2014, the date the Data Breach began, through July 15, 2015, the last date on which Anthem provided information to the Examination Team. The Examination was conducted under the authority of the Examination Statutes.

The Examination Team did not conduct an independent investigation of the Data Breach. Instead, the Lead States directed that the Examination Team review the suitability of Anthem's systems and security protocols prior to the breach, its reaction to the Data Breach, and subsequent efforts to address system security and remediate consumer impacts. The Examination therefore included both elements of independent examination and peer review regarding the work performed by Anthem and its retained cybersecurity vendor, Mandiant.

The Examination Team's work included four principal phases: (i) Integration; (ii) Initial Assessment; (iii) Breach Assessment; and (iv) Cybersecurity Assessment. The key elements of each phase included:

#### *Integration*

- Meet with key Anthem personnel, representatives of the Lead States, and the Examination Team
- Provide an initial data request to Anthem

- Develop protocols for communication, information flow, documentation, and reporting

#### *Initial Assessment*

- Interview key Anthem and Mandiant personnel to orient the Examination Team to the Data Breach and Anthem's response
- Obtain technical documents and materials associated with Anthem's pre-breach cybersecurity environment, its response to the Data Breach, and the efforts that took place post-breach to assess vulnerabilities in Anthem's cybersecurity program

#### *Breach Assessment*

- Review Anthem's technical scoping of the Data Breach, the analysis that was conducted, and the technical and business conclusions reached
- Review the actions taken by Anthem and Mandiant to detect, contain and respond to the Data Breach, including consumer protections

#### *Cybersecurity Assessment*

- Conduct an in-depth review of the cybersecurity controls that were in place prior to the Data Breach and the controls that are currently in place
- Perform an external limited-in-scope penetration test to determine whether Anthem's controls appeared to be effective to detect and/or prevent another breach using tactics, techniques, and procedures similar to those used by the Attacker perpetrating the Data Breach

The Examination Team began work in May of 2015, and submitted a draft confidential report on July 20, 2015 (the "Confidential Report"). The Examination Team discussed its findings and conclusions with the Lead States.

### **Examination Findings**

This examination report is intended for public distribution and, accordingly, does not reflect all findings, analysis and information contained in the Confidential Report as the Confidential Report contains confidential and proprietary information. This examination report summarizes the points necessary to understand what occurred and to answer the regulatory questions giving rise to the Examination Purpose. This examination report is subject in all

respects to the limiting conditions described in the attached appendix entitled “Limitations of Report.” The examination findings are presented below in six sections: The Data Breach, Pre-Breach Cybersecurity, Pre-Breach Response Preparation, Response Adequacy, Post-Breach Cybersecurity, and Corrective Actions.

*The Data Breach* – Anthem discovered the Data Breach on January 27, 2015, and immediately informed the Federal Bureau of Investigation that it was investigating a potentially serious security breach. Anthem also engaged Mandiant to assist the Company with its post-breach response. The Company implemented its Incident Response Plan (“IR Plan”), and the last successful malicious activity was noted by Anthem on January 30, 2015. Subsequent investigation by the Company and Mandiant determined that the Data Breach began on February 18, 2014, when a user in Anthem’s Amerigroup subsidiary opened an e-mail (commonly referred to as a “phishing” e-mail) containing malicious content. Opening this e-mail permitted the download of malicious files to the user’s local system, allowing the Attacker to gain remote access to that computer.

Starting with the initial remote access, the Attacker was able to move laterally (across Anthem systems) and escalate privileges (gain increasingly greater ability to access information and make changes in Anthem’s environment). The Attacker utilized at least 50 accounts and compromised at least 90 systems within the Anthem enterprise environment including, eventually, the Company’s enterprise data warehouse – a system that stores a large amount of consumer personally identifiable information (“PII”). Queries to that data warehouse resulted in access to an exfiltration of approximately 78.8 million unique user records.



Examination Team members from CrowdStrike determined the identity of the Attacker with high confidence.<sup>1</sup> CrowdStrike also concluded with medium confidence that the Attacker was acting on behalf of a foreign government. In CrowdStrike's experience, attacks associated with this foreign government have not resulted in PII being transferred to non-state actors.

*Pre-Breach Cybersecurity* – The Examination Team evaluated whether Anthem had in place, prior to the Data Breach, a cybersecurity program suitable for a company of its size, operations, and business purpose. In our view, Anthem appeared to have taken reasonable measures prior to the Data Breach to protect its computer network and data. Those measures included the implementation of cybersecurity technologies and procedures consistent with or exceeding those of a typical organization of its size and type. However, the Attacker was able to exploit certain cybersecurity gaps which allowed the Data Breach to occur.

*Pre-Breach Response Preparation* - Our review disclosed that prior to the breach the Company had a detailed IR Plan in place. The IR Plan documented roles, responsibilities, and processes related to incident response, and those procedures had been tested in several “tabletop” exercises prior to the Data Breach.

*Response Adequacy* – The Examination Team investigated whether Anthem's execution of the IR Plan resulted in a rapid and effective response to the Data Breach. Our review determined that, once the breach was detected, Anthem's cybersecurity personnel immediately involved top management, took immediate investigative action to ascertain the magnitude of the breach, and took remediation steps to contain the breach. The Company also communicated with

---

<sup>1</sup> For purposes of attacker attribution, CrowdStrike's confidence assessments were based on: **High** - Information on the subject is of high quality from multiple sources or from a single highly reliable source, and the nature of the issue makes it possible to render a solid judgment; **Medium** - Information on the subject is interpreted various ways, alternating views exist, or the information, while credible, is of insufficient reliability to warrant a higher level of confidence; and **Low** - Information on the subject is scant, questionable, or very fragmented; it is difficult to make solid analytic inferences; or significant concerns or problems with the source exist.

law enforcement officials, regulators, and the public in a timely manner. Anthem's response to the Data Breach therefore appeared to be timely and effective, and removed the Attacker's ability to access the network within three days of identifying the Data Breach.

*Post-Breach Cybersecurity* – Following the Data Breach, Anthem engaged Mandiant to investigate the Data Breach, assess the adequacy of its cybersecurity controls, and recommend steps to improve its security posture. Anthem advised the Examination Team that it had implemented two-factor authentication on all remote access tools, deployed a "Privileged Account Management" solution, and added enhanced additional logging resources to its existing security event and incident management solutions. Further, the Company conducted a complete reset of passwords for all privileged users, suspended all remote access pending implementation of two-factor authentication, and created new Network Admin IDs to replace existing IDs. Going forward, Anthem acquired additional technology to improve its monitoring capabilities in critical databases.

The Examination Team noted exploitable vulnerabilities in the immediate aftermath of the Data Breach, and that Anthem had developed a remediation plan to address those issues. It is the Examination Team's view that Anthem's improvements to its cybersecurity protocols and schedule of planned future improvements appeared to be reasonable efforts to secure the environment beyond the initial Data Breach remediation tasks.

*Corrective Actions* – After discovering the Data Breach, Anthem promptly communicated and cooperated with law enforcement and regulatory officials. The Company also notified the public and affected individuals through direct mail, e-mail, news publications, website notice, and working with state insurance departments. Within two weeks of discovering the Data Breach, the Company also engaged a consumer credit protection company to provide

credit protection services to all breach-affected consumers. Anthem provided credit protection services for a two-year period. Anthem's consumer protections were at least equal to those afforded to consumers in the other breach situations with which the Examination Team was familiar.

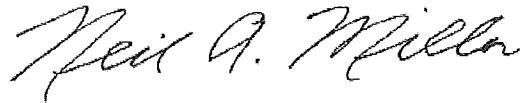
### **Summary**

The Attacker exploited weaknesses in Anthem's information security processes and technology to access and exfiltrate a large quantity of Anthem customer data. Once the Data Breach was identified, Anthem responded quickly and effectively to the Attacker's presence in its network, fully removing the Attacker's access to the network within three days. While deficiencies within Anthem's cybersecurity posture were noted by the Examination Team, these deficiencies were not, in our experience, uncommon to companies comparable to Anthem in size and scope. While the pre-breach deficiencies impacted Anthem's ability to reduce the likelihood of and quickly detect the Data Breach, the controls implemented subsequent to the Data Breach should improve Anthem's ability to detect future breaches and enable Anthem to respond more effectively to a future attack than was the case in this instance.

### **Verification and Report Submission**

The foregoing is a true and accurate report of the Examination. The report of examination is herewith respectfully submitted.

Sincerely,



---

Neil A. Miller  
Examiner-in-Charge  
Alvarez & Marsal Insurance and Risk Advisory  
Services, LLC

### **Acknowledgement**

The Examination Team extends our sincere thanks and appreciation to Commissioner Robertson and his staff at the Indiana Department of Insurance for their leadership and facilitation of this examination. We also wish to thank the other Lead States for their leadership and assistance on this examination.

The Examination Team further acknowledges and thanks Anthem for all of their work in facilitating this examination, and for the courtesies they extended to us throughout this examination.

## **Appendix - Limitations of Report**

This report and the information contained herein (“Information”) has been prepared solely for use by the Indiana Department of Insurance (“IDOI”), other Lead States and participating jurisdictions (the “Intended Recipients”).

The Examination Team assumes no duties or obligations to any recipient of this report by virtue of their access hereto save as set forth in a separate written agreement between the Examination Team and such recipient. The limiting conditions and disclaimers set forth herein are an integral part of this report, must be reviewed in conjunction herewith, and may not be modified or distributed separately. Any use or potential publication of this report is not intended nor should it be construed as a waiver of any privilege or immunity from disclosure that may attach to the Examination Team’s privileged work, investigation, and reports.

This report has been prepared and compiled as a summary of the Examination Team’s efforts to assist the IDOI in evaluating issues related to the cybersecurity breach of Anthem and does not purport to contain all necessary information that may be required to evaluate the Data Breach and response, regardless of how pertinent or material such information may be. The scope of the examination did not include verification of any of the underlying source data which provides a basis for the descriptions and findings in the report. Accordingly, the Examination Team makes no representation or warranty as to the accuracy, reliability or completeness of the information. No member of the Examination Team is responsible to any party, in any way, for any representation, analysis, or findings contained in the report, or the manner in which the report may be used.

This report and any related advice or Information is provided solely for the use and benefit of the Intended Recipients and only in connection with the purpose in respect of which

the services are provided. In no event, regardless of whether consent has been provided, shall the Examination Team assume any responsibility, liability or duty of care to any person or entity other than the IDOI and Lead States. This report does not take account of those matters or issues which might be of relevance to any entity or person. The Examination Team has not considered any such matters or issues, and any third party is responsible for conducting its own investigation with respect to the Information and any related transactions or activities. The Examination Team makes no representations or warranties, express or implied, to any third party on which any such party may rely with respect to the Information, including without limitation, as to accuracy or completeness, the inclusion or omission of any facts or information, or as to its suitability, sufficiency or appropriateness for the purposes of any such party.

This report serves as a point-in-time assessment of the Anthem environment. Any and all security controls or processes that are implemented after the examination was completed are considered outside the scope of the assessment.



To the Parent(s) or Guardian(s) of:  
MINOR'S NAME  
ADDRESS  
CITY, ST ZIP

<DATE>

## **NOTICE OF OFFER FOR MINORS RELATING TO CYBER ATTACK ON [ANTHEM]**

Dear Parent(s) or Guardian(s) of <Minor's Name>:

In 2015, you may have received a letter about a potential impact on your child's personal information from a cyber-attack on [Anthem, Inc.] [Anthem] has been asked by state insurance commissioners to offer to pay for a [credit freeze/block] for your child.

**Please note:** This is **NOT** a notice of a new attack. There isn't any evidence of child or adult identity theft from the cyber-attack. This is simply to tell you about an offer [Anthem] was asked to make.

### **What's a [credit freeze/block]?**

A [credit freeze/block] will help to prevent banks, credit card companies and others from opening new credit accounts in your child's name without your OK. It will help prevent fraudulent accounts from being opened with your child's information. It can also help to prevent others from getting information from your child's credit report, if they have one. Anthem will pay for the [credit freeze/block] at the national credit bureaus that put the [credit freeze/block] in place.

### **Why is [Anthem] making this offer?**

We're making this offer to give additional services to minors. The state insurance commissioners asked us to pay for a [credit freeze/ block] with these national credit bureaus:

- Equifax
- Experian
- Transunion

We'll pay now for the fee to place and remove the [credit freeze/block]. This way when you want to permanently remove the [credit freeze/block] in the future, it will already be paid for.

### **Who's eligible?**

Individuals who were:

- Younger than 18 years old on February 5, 2015 and
- Possibly impacted by the 2015 cyber-attack

### **How do I place a [credit freeze/block] for my child?**

Follow the steps [below or attached]. [Anthem] will get the bill from the credit bureaus. You won't need to pay.

**How long does this offer last?**

You have one year from the date of this letter to place the [credit freeze/block].

**Do I have to place a [credit freeze/block]?**

No. It's your choice if you want to place one for your child.

**What if I already placed a [credit freeze/block] for my child?**

If you already placed and paid for a [freeze/block] for your child on or after February 5, 2015, [Anthem] will pay you back. Go to [www.AnthemFacts.com] or call <toll-free phone number> for help.

**What if my child is an adult now? Can he or she get this offer?**

No, this offer is only for those younger than 18 years old now. If you already paid for a [freeze] on or after February 5, 2015, we'll pay you back.

**Have questions?** Go to [www.AnthemFacts.com] or call <toll-free phone number>.

Si necesita esta correspondencia en español, llame al [XXX-XXX-XXXX] o [TTY/TDD XXX-XXX-XXXX]

<INSTRUCTIONS TO BE FINALIZED ONCE PROCESS WITH CREDIT BUREAUS IS FINALIZED. >

**Targeted Multistate Market Conduct and Financial Examination**

of

Anthem Insurance Companies, Inc.

Regulatory Settlement Agreement

**PARTICIPATING REGULATOR ADOPTION**

On behalf of \_\_\_\_\_ Idaho Department of Insurance \_\_\_\_\_,

I, \_\_\_\_\_ Dean L. Cameron \_\_\_\_\_, hereby adopt, agree and approve the

Anthem Regulatory Settlement Agreement dated December 14, 2016.

Idaho Department of Insurance

By:

Dean L. Cameron

Title:

DIRECTOR

Date:

12/14/16

**EXHIBIT**

2

tabbles